Comprehensive Auditing and Identity-Based Data Outsourcing in Cloud.

Harshada Salunkhe[1],Kavita Nabage[2], Shivani Waghmare[3], Pradip Ugale[4]

1 Student, Computer Engineering, SPCOE, Maharashtra, India
2 Student, Computer Engineering, SPCOE, Maharashtra, India
3 Student, Computer Engineering, SPCOE, Maharashtra, India
4Assistant professor, Computer Engineering, SPCOE, Maharashtra, India

ABSTRACT

More and more clients would like to store their data to public cloud servers (PCSs) along with the rapid development of cloud computing.. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data are kept intact without downloading the whole data. From the security problems, we propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: identity based proxy-oriented data uploading and remote data integrity checking in public cloud .We give the formal definition, system model, and security model. Then, a protocol is designed using the bilinear pairings. The proposed protocol is provably secure based on the hardness of computational DiffieHellman problem. Our protocol is also efficient and flexible. Based on the original client's authorization, the proposed protocol can realize private remote data integrity checking, delegated remote data integrity checking, and public remote data integrity checking

Keyword : *Security, PKG, IB, Encryption algorithm. ,PCS*
….

1. 1. Introduction

Identity based public key system (ID-PKS) is an alternative for public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. An ID-PKS setting consists of trusted third party (i.e. private key generator, PKG) and a users. The PKG is responsible to generate each users private key by using the associated ID information (e.g.name, e-mail address, or social security number). so, requirement of certificate and PKI are not necessary in the associated cryptographic mechanisms under ID-PKS settings. ID-based encryption (IBE) allows a sender to encrypt message directly by using a receivers ID without checking the validation of public key certificate. Accordingly, the receiver uses the private key associated with her/his ID to decrypt such cipher text. Since a public key setting has to provide a user revocation mechanism, there search issue on how to revoke misbehaving or compromised users in an ID-PKS setting is naturally raised. In conventional public key settings, certificate revocation list (CRL) is a known revocation approach. In the CRL approach, if a party receives a public key and its associated certificate, she/he first validates them and then looks up the CRL to ensure that the public key has not been revoked. In such a case, the procedure requires the online assistance under PKI so that it will incur communication bottleneck. To improve the performance, several efficient revocation mechanisms for conventional public key settings have been we studied for PKI. Indeed, researchers also pay attention to the revocation issue of ID-PKS Settings.

1.1 Motivation

Due to the complexity and volume, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access. Nevertheless, verifying the access legitimacy of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical

challenges to make cloud-based big data storage practical and effective. Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this paper, we propose a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds. We first propose a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU, and then detail our scheme and analyze its correctness, security strengths, and computational efficiency.

1.2 LITERATURE SURVEY

D. Boneh and M. Franklin, To propose a fully functional Secure Encryption scheme (SECURE CHANNEL). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie Hellman problem. System is based on bilinear maps between groups. The KG in the scheme can be distributed so that the master-key is never available in a single location. Unlike common threshold systems, shows that robustness for our distributed KG is free. [1]

R. Housley, W. Polk, W. Ford, and D. Solo, This memo profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. An overview of this approach and model is provided as an introduction. The X.509 v3 certificate format is descrSecure Channeld in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are descrSecure Channeld and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is descrSecure Channeld in detail along with standard and Internet-specific extensions. An algorithm for X.509 certification path validation is descrSecure Channeld. An ASN.1 module and examples are provided in the appendices. [2]

2. Problem Statement

The Problem is to determine how to handle Remote Data Integrity Checking as well as isolate Anonymous & Anonymous Control User.

2.1 Goals And Objective

- Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modelling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices

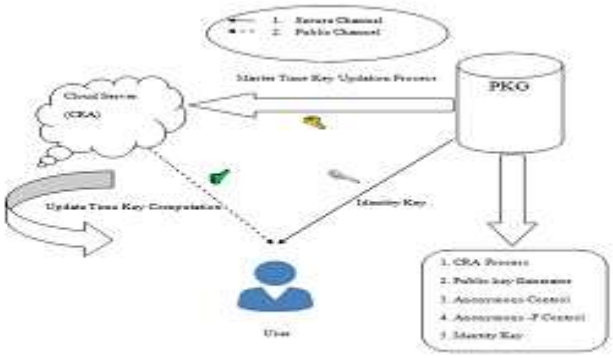
2.2 Existing System

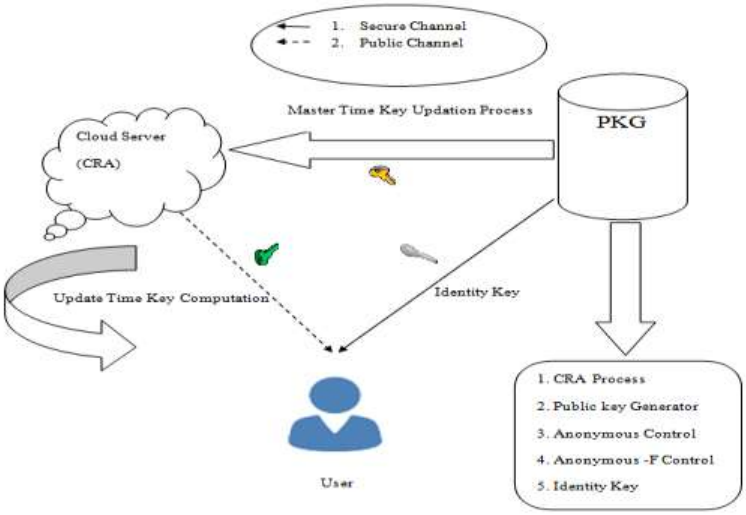
1. More and more clients would like to store their data to PCS (public cloud servers) along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data is kept intact without downloading the whole data.
2. Secure Encryption (IB) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.
3. To suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period.
4. To way for users to periodically renew their private keys without interacting with KG.

5. To space efficient revocable SECURE CHANNEL mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where is the number of revoked users.

2.3 Proposed System

- To Proposed that easily isolate authorized user & un-authorized user.
- Expiration key maintain Time session process.
- Data manipulation easily possible.
- Upload any type of file.
- Grouping clause proper manage





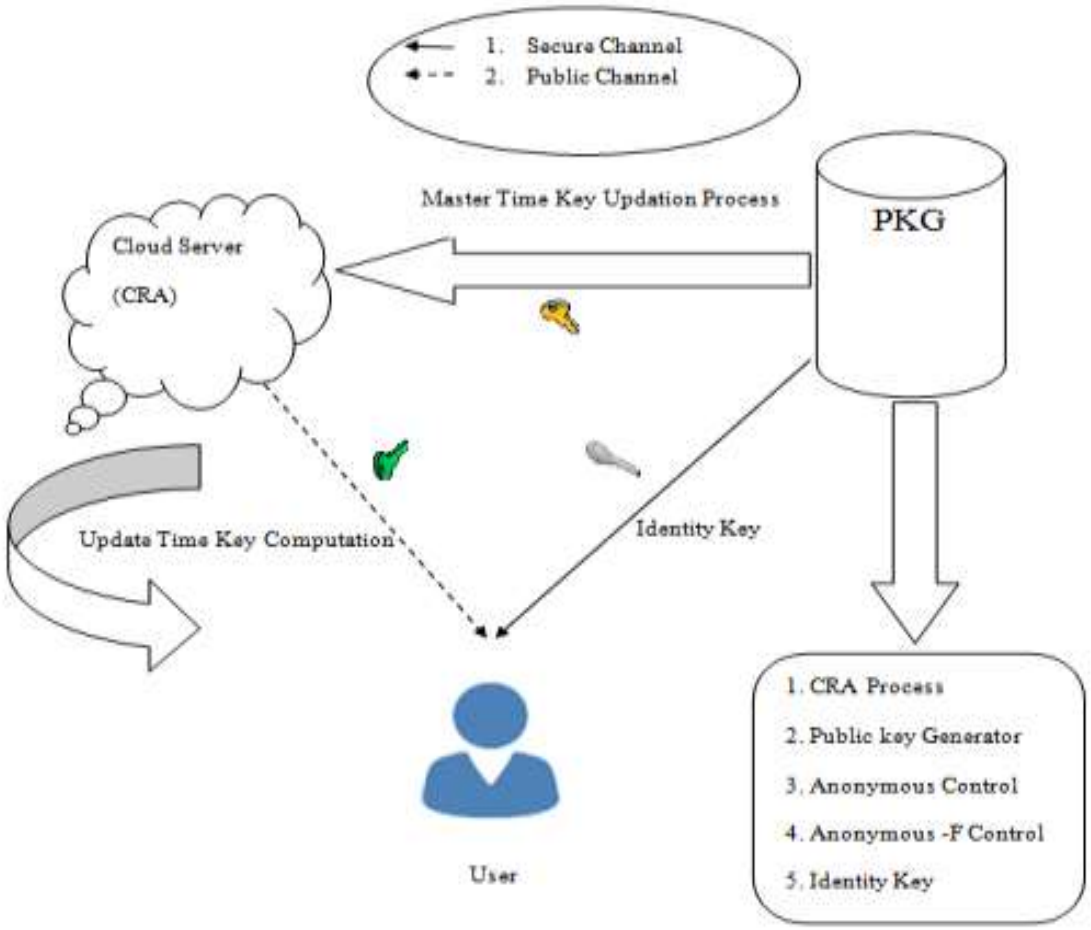


Fig1.System Architecture

2.4 Application

- To Propose a new revocable SECURE CHANNEL Technique with a cloud revocation authority (VERIFIER).
- To solve the two shortcomings namely, computation and communication costs and lack of scalability.
- To introduce a cloud revocation authority (VERIFIER) to replace the role of the KU-CSP in Li et al.'s scheme.
- It is evident that our scheme solves the un-scalability problem of the KU-CSP.

3. Mathematical Model

- Set Theory Analysis

U (Z) = {u1, u2,u3.....un}
F (Z) = {f1, f2,f3.....fn}
S (Z) = {s1, s2,s3.....sn}
MAC (Z) = {m1,m2,m3....mn}

D (Z) = {d1, d2,d3.....dn}
Where
U (Z): Total number of users.
F (Z): Total number of files.
S (Z): Total number of secret key(update Time key)
MAC (Z): Master key.
D (Z): Total data

a) Uploading file: U (Z) U F(Z): S(Z) U MAC(Z) :-

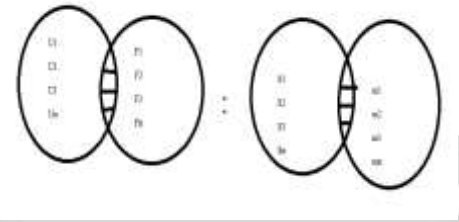


Fig. Uploading files

User is file upload using Standard algorithm to create secret key as well as master key.

b) Downloading Files : U (Z) U S(Z) U MAC(Z) : D(Z) :-

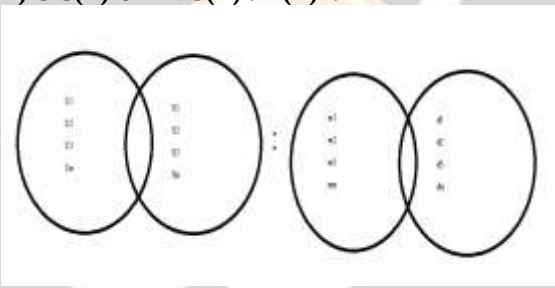


Fig.downloading files

User is file upload using Standard algorithm to create secret key as well as master key. Every key is change. when file download with the help of VERIFIER.

Success Condition: Properly Maintain key

Failure Condition: Anonymous User & Anonymous-F User Maintain Authorization

3.1 Use Case Diagram, Sequence Diagram

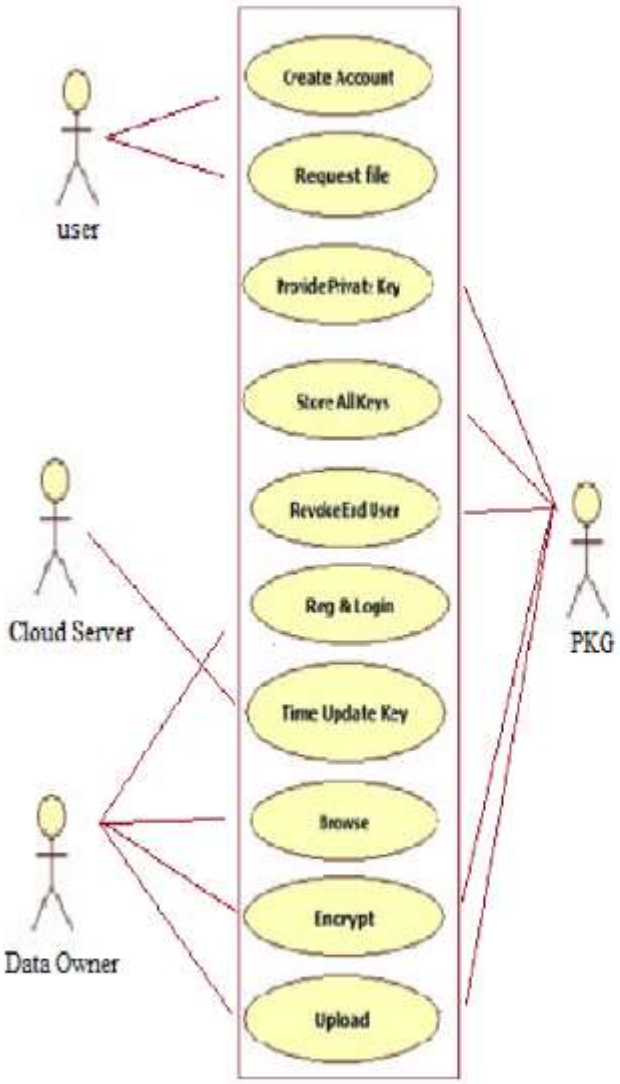


Fig -2: Use Case Diagram

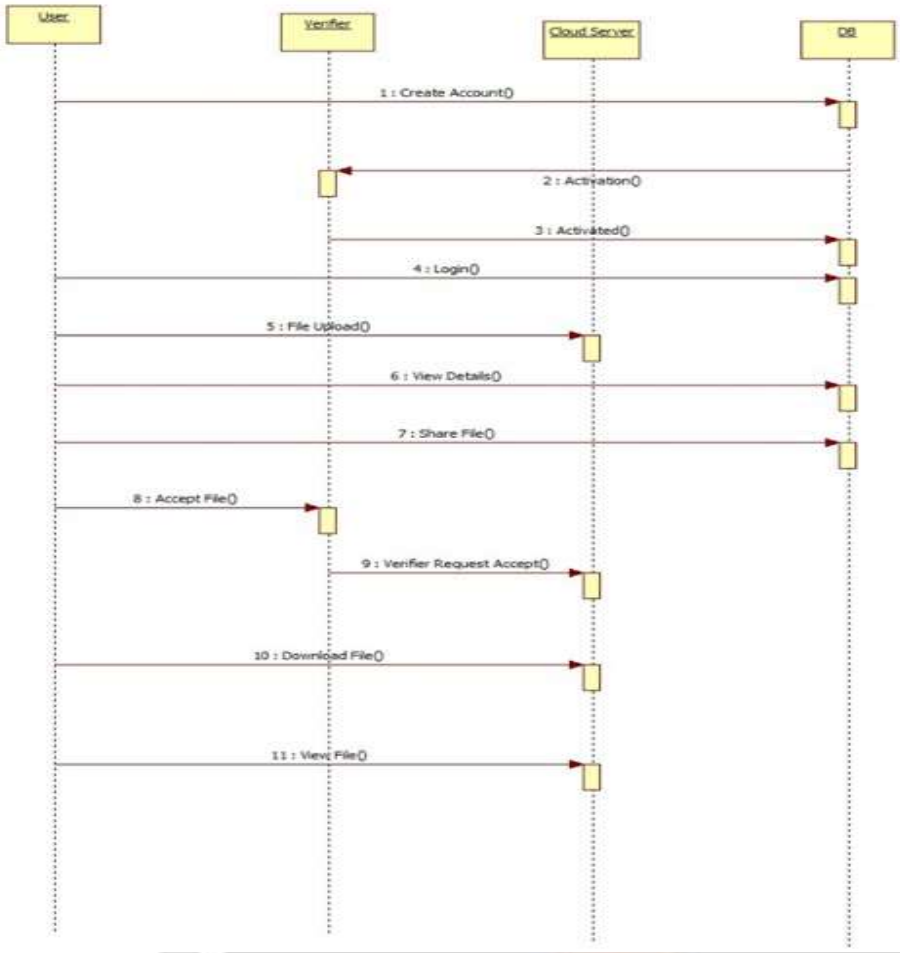


Fig: Sequence Diagram

4. CONCLUSIONS

Finally, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU and then present a secure and verifiable access control scheme based on the improved NTRU to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud.

5. ACKNOWLEDGEMENT

I would like to thanks to my project guide **Prof**. **Ugale P. R.** Who always being with presence & constant, constructive criticism to make this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

6. REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," *Stamford, CT: Gartner*, 2012.
[2] V. Marx, "Biology: The big challenges of big data," *Nature*, vol. 498, no. 7453, pp. 255–260, 2013.

[3] S. Galbraith,I. Blake, G. Seroussi and N. Smart , "Advances in Elliptic Curve Cryptography," Cambridge University Press,2005.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances in Cryptology–EUROCRYPT 2005*, pp. 457–473,2005.
[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*. ACM, 2013, pp. 31–36

BIOGRAPHIES (Not Essential)

Author Photo-1 	**Salunkhe Harshada** She is currently learning BE degree in computer engineering From Pune University, She research interests include Comprehensive Auditing and Identity-Based Data Out sourcing in Cloud
Author Photo-2 	**Nabage Kavita** She is currently learning BE degree in computer engineering From Pune University, Her research interests include Comprehensive Auditing and Identity-Based Data Out sourcing in Cloud
Author Photo-3 	**Waghmare Shivani** She is currently learning BE degree in computer engineering From Pune University, Her research interests include Comprehensive Auditing and Identity-Based Data Out sourcing in Cloud .